

Service: Desktop Intrusion Prevention Software

Service Line: LAN and Desktop Services

Status: In production

General Description:

This GTA product provides customers with software that provides preemptive security protection for desktops and laptops with the following protection and features:

- Spyware prevention
- Virtual patching
- Intrusion prevention
- Application protection
- Anti-virus awareness
- Virus prevention
- Memory protection
- Firewall
- Automatic updates

The Desktop Intrusion Prevention Software Product is **installed and managed by the customer**.

Service Level Targets:

Established by the customer's operations personnel.

Availability:

Established by the customer's operations personnel.

Limitations:

- Designed **only** for use with a desktop running an operating system of Windows 2000 or Windows XP. The product will not work with Linux or any other operating system.
- Only works with Microsoft SQL.

Prerequisites: None

Pricing / Charges:

The rate for fiscal year 2006 and 2007 and for budgeting for fiscal 2008 is 83 cents per seat per month. This covers the customer's annual per seat software maintenance fee that the vendor charges the State.

Service Components or Product Features Included in Base Price:

- Management Console software downloaded by agency from www.ISS.net
- 24 hours of GTA consultation for customer implementation

Options Available for an Additional Charge: N/A

Service Components or Product Features Not Included: N/A

What GTA Provides:

- License keys for the number of clients the customer orders
- Billing for the number of clients the customer orders
- 24 hours of implementation consulting

What the Customer Provides:

- Server hardware
- SiteProtector centralized management console (downloaded from www.iss.net)
- Security Agent configuration and deployment planning
- Vendor training for internal staff
- Management for the desktop security service
- Maintenance and tracking of all Operating Environment (OE) Upgrades, patches and licenses in order to consistently achieve the desired service levels
- Performance tuning, monitoring, reporting and system-level troubleshooting of the software
- Incident, change, problem and request management reporting and tracking
- Authorizing/rescinding authorization of Desktop Client installations
- Vaulting of security data as prescribed by federal and Georgia law and customer requirements
- Managing backup and recovery
- Obtaining the necessary internal business case approvals for the initial desktop security policy, and for any subsequently requested changes to that same policy
- Maintaining escalation and notifications paths and contact information for communicating about incidents associated with the service

Service Support:

- **GTA provides** customer access to the vendor's third level support. GTA will provide the customer with vendor contact information during the implementation consulting.
- **The customer provides** first and second level problem resolution support.

Service Issue Escalation:

- **GTA provides** escalation to the vendor for third level problem resolution support. GTA will provide customers with specific escalation information during implementation.
- **The customer provides** Help Desk functionality and appropriate agency internal service escalation procedures.

Benefits / Advantages:

- Provides valuable insight to the frequency and types of security threats affecting the customer's desktops. As part of the Desktop Intrusion Prevention Software, customers will be able to generate any of 33 canned reports (see the "Other Information" section for the report list) using the SiteProtector management console. These reports will provide customers with the information required to make the strategic decisions necessary to limit their exposure to desktop security threats.
- Proactively blocks spyware and more than 97% of new and unknown viruses and worms — without an update. The Desktop Intrusion Prevention Software provides advanced virus protection because, rather than relying on signatures for detection, it uses a behavioral system that analyzes the activities of an executable file and detects whole families of malicious code.
- Easy to manage and scales for small to very large deployments. Using a centralized management system, GTA administrators can control 100,000 Desktop Intrusion Prevention Software agents from a single console.
- ISS provides continuous updates to the security protection. These and any configuration modifications are automatically pushed to desktop security agents when they connect to the central management console (requires Internet access).
- Provides location-based protection by automatically enabling additional security when a laptop enters a foreign or untrusted network, such as a wireless connection in a coffee shop. This reduces the possibility of these laptops introducing threats to their corporate environments.
- Blocks buffer overflow attacks, which account for a significant portion of all high-risk vulnerabilities. Like a circuit breaker, it automatically trips to protect the system the instant malicious code tries to run.
- Can be used to ensure that users have compliant systems or are running protective software, like the desktop agent or anti-virus, before allowing local access to the corporate network or remote access through a virtual private network (VPN). It can also prevent users from running or even installing banned programs.

- Fits seamlessly within the customer's existing corporate infrastructure and works with Active Directory, most e-mail and web clients, and popular anti-virus and VPN software.

How to Start this Service:

Customers should contact the GTA Office of Solutions Marketing at gtasolutionsmrktg@gta.ga.gov or (404) 651-6964 to be put in touch with their GTA Account Manager.

Related Services and Products: None

Other Information: Standard Reports List:

Assessment Reports:

- Operating System Summary: Displays percentage and number of hosts by operating system discovered during an automated network scan.
- Vulnerability Counts: Lists detected vulnerabilities by total number and by percentage.
- Host Assessment Summary: Lists discovered hosts and for each host, identifies network services and vulnerabilities.
- Host Assessment Detail: Detailed list of vulnerabilities and services for each host, including vulnerability remedies and references.
- Operating System Summary by Host: List of hosts scanned and their operating system.
- Service Summary by Host: List of services discovered for each host scanned.
- Vulnerability Counts by Host: Count of vulnerabilities discovered for each host by severity.
- Vulnerability Remedies by Host: List of vulnerabilities and their remedies for each host.
- Vulnerability Names by Host: List of vulnerability names for each host.
- Service Summary: List of services discovered.
- Top Vulnerabilities: Lists the top vulnerabilities by frequency for a specified group and time.
- Vulnerability Summary by Host: List of vulnerabilities and their descriptions for each host.
- Vulnerability Detail by Host: Detailed list of all vulnerability information available for each host.
- Vulnerability by Group: Compares vulnerabilities across subgroups of a selected group.
- Vulnerability by Host: Lists the top hosts by number of vulnerabilities for a specified group and time.
- Vulnerability by OS: Compares vulnerability counts by operating systems.

Attack Activity Reports

- Attacks by Group: Compares attack counts across subgroups of a selected group.
- Top Attacks: Lists the top attack names by frequency for a specified group and time.
- Top Sources of Attacks: Lists the top attack sources by frequency for a specified group and time.
- Top Targets of Attacks: Lists the top attack targets by frequency for a specified group and time.

Audit Reports

- Audit Detail: Provides an audit trail of significant actions performed by SiteProtector users.

Compliance Reports

- Server Protection Report: Displays counts of servers protected and not protected with version details.

Content Filtering Reports

- Top Web Categories: Lists categories with the number of hosts and requests.
- Web Requests: Count of Web requests by category or client.

Desktop Reports

- Desktop Protection Report: Displays counts of hosts protected and not protected with version details.

Management Reports

- Attack Incidents: Lists all attack incidents created for a specified time.
- Attack Status Summary: Displays attack status summary including Security Fusion and blocked events.
- Attack Trend: Attack activity by day/week/month/quarter/year.
- Virus Activity Trend: Virus activity by day/week/month/quarter/year.
- Vulnerability Trend: Vulnerabilities by day/week/month/quarter/year.

Virus Activity Reports

- Top Virus Activity: Lists the top viruses by frequency for a specified group and time.
- Virus Activity by Group: Compares virus activity across subgroups of a selected group.
- Virus Activity by Host: Lists the top hosts by amount of virus activity for a specified group and time.